Attorney Docket: YO999-411

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Kanevsky et al.
Docket No.: YO999-411
Serial No.: 09/437,352
Filing Date: November 9, 1999
Group: 2132
Examiner: Cas P. Stulberger

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature: Judy Muzyka Date: April 7, 2005

Title: Methods and Apparatus for Verifying the Identity of a User Requesting Access Using Location Information

---

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

1. Appeal Brief; and
2. Copy of Notice of Appeal, filed on February 3, 2005, with copy of stamped return postcard indicating receipt of Notice by PTO on February 7, 2005.

There is an additional fee of $500 due in conjunction with this submission under 37 CFR §1.17(c). Please charge **IBM Corporation's Deposit Account No. 50-0510** the amount of $500 to cover this fee. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **IBM Corporation's Deposit Account No. 50-0510** as required to correct the error. A duplicate copy of this letter is enclosed.

Respectfully,

Kevin M. Mason

Date: April 7, 2005

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Kanevsky et al.
Docket No.: YO999-411
Serial No.: 09/437,352
Filing Date: November 9, 1999
Group: 2132
Examiner: Cas P. Stulberger

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature: Judy Murzyk Date: April 7, 2005

Title: Methods and Apparatus for Verifying the Identity of a User Requesting Access Using Location Information

---

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby appeal the final rejection dated December 6, 2004, of claims 1 through 58 of the above-identified patent application.

REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, as evidenced by an assignment recorded on January 24, 2000 in the United States Patent and Trademark Office at Reel 010511, Frame 0772. The assignee, International Business Machines Corporation, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1 through 58 are pending in the above-identified patent application. Claims 1-11, 13, 15-21, 24, 26-32, 35, 37-39, 40-47, 49, and 50-57 remain

rejected under 35 U.S.C. §103(a) as being unpatentable over Li et al. (United States Patent Number 6,219,793 B1), and further in view of MacDoran et al. (United States Patent Number 5,757,916). Claims 12, 14, 22, 23, 25, 33, 34, 36, 48, and 58 remain rejected under 35 U.S.C. §103(a) as being unpatentable over Li et al. in view of MacDoran et al., and further in view of "Wireless Enhanced 9-1-1 Service – Making it a Reality," Bell Labs Technical Journal (Autumn 1996) by Meyer et al. (hereinafter Meyer et al.)

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to a global positioning system (GPS)-based access control method and apparatus for limiting access to a device or secure facility by verifying the location of an authorized user. The GPS-based access control system confirms that the user requesting access to a device or secure location is physically present at the location of the device or secure location (page 4, line 19, to page 6, line 25). Upon an access control request, the location of the user is obtained using an individual GPS system carried by each user on a portable device, such as a pocket token, computer-readable card, cellular telephone or watch. If the location of a person making an access control request does not coincide with the coordinates of the individual GPS that is being worn by the authorized user associated with the password, then the person requesting access is unauthorized (page 6, line 26, to page 8, line 17).

STATEMENT OF GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-11, 13, 15-21, 24, 26-32, 35, 37-39, 40-47, 49, and 50-57 are rejected under 35 U.S.C. §103(a) as being unpatentable over Li et al., and further in view of MacDoran et al.; and claims 12, 14, 22, 23, 25, 33, 34, 36, 48, and 58 are rejected under 35 U.S.C. §103(a) as being unpatentable over Li et al. in view of MacDoran et al., and further in view of Meyer et al.

ARGUMENT

Rejection Under 35 U.S.C. §103(a) as Being Unpatentable Over Li et al., and Further in View of MacDoran

Independent Claims 1, 16, 27, 38, 39, 42, 45, 49, 52 and 55

Independent claims 1, 16, 27, 38, 39, 42, 45, 49, 52, and 55 are rejected under 35 U.S.C. §103(a) as being unpatentable over Li et al., and further in view of MacDoran.

In particular, the Examiner asserts that Li teaches a challenge-response to authenticate a wireless communication, but acknowledges that Li does not disclose a "challenge response method that uses the location." The Examiner asserts, however, that MacDoran discloses a "method of providing the location of the client ...and granting access to the user if the location is within a predetermined threshold." In the Response to Arguments section of the final Office Action, the Examiner asserts the following points:

4. MacDoran discloses that the LSS device can also be configured into a single microchip for integration into original equipment manufactured products (col. 15, lines 43-47 and 58-59) and that this allows each user to have a separate GPS device.

5. MacDoran discloses authentication (of) a user or device by using various methods such as passwords, PIN's, smart cards, PCMCIA cards, and biometric authentication (col. 1, lines 21-55), and that this meets the limitation of authenticating an individual person.

6. Although MacDoran discloses that "the definition does not extend to individual users that operate an entity, because the invention does not have the ability to authenticate an individual person," does not mean that creating a system that can authenticate an individual user is therefore not taught by MacDoran.

7. MacDoran discloses the "host authentication server produces a remote client location that matches the previously registered client location within a predetermined threshold, such as 3 meters, access is granted to the remote client user" (col. 24, lines 18-29).

8. MacDoren discloses comparing the location of the client with the location stored in the database (col. 24, lines 14-16).

9. The Examiner asserts that, "in order to biometrically authenticate the user has to be present at the location of the transmitting device or else it would be impossible to accomplish any of the previously described biometric authentication techniques."

10. Meyer discloses "using 911 techniques or querying the user about something at the location of a requested device or facility."

Applicants note that MacDoran is directed to a method and apparatus for authenticating the identity of a remote user *entity* where the identity of such user entity is authenticated by use of information specific to geodetic location of the user *entity* (see, Abstract). MacDoran compares the *expected location of an electronic device* with the *current location of the device* and will not allow access if the locations do not match. The present invention, alternatively, is directed to authenticating a user by confirming the location of the user utilizing, for example, a GPS device carried by the user. Thus, MacDoran would require a *single GPS device located at a client machine* and the present invention would require, for example, a *separate GPS device for each user* of the client machine.

Applicants also note that MacDoran defines "entity" as an electronic device and specifically states that this definition "*does not extend to individual users* that operate an entity, because the invention does *not* have the ability to authenticate an individual person." (Col. 6, lines 59-65; emphasis added.) Thus, MacDoran actually teaches away from the present invention by teaching that the invention cannot be used to authenticate an individual person.

Independent claims 1, 16, 27, and 38 require identifying *a location of an authorized person* associated with said response; identifying a location where said response is received; and *providing access to said user* if said locations match. Independent claims 39 and 49 require identifying each registered person within a predefined distance of said requested device. Independent claims 42 and 52 require *identifying said user* by comparing a *location of each identified potential user* with a location where said biometric information was obtained. Independent claims 45 and 55 require *identifying said user* and *confirming said user requesting access to said device is*

physically present at the location of said requested device by determining a location of said transmitting device (wherein said transmitting device is associated with said user). MacDoran does not disclose or suggest any of these limitations.

Thus, Li and MacDoran, alone or in combination, do not disclose or suggest identifying a location of an authorized person associated with said response; identifying a location where said response is received; and providing access to said user if said locations match, as required by independent claims 1, 16, 27, and 38, do not disclose or suggest identifying each registered person within a predefined distance of said requested device, as required by independent claims 39 and 49, do not disclose or suggest identifying said user by comparing a location of each identified potential users with a location where said biometric information was obtained, as required by independent claims 42 and 52, and do not disclose or suggest identifying said user and confirming said user requesting access to said device is physically present at the location of said requested device by determining a location of said transmitting device (wherein said transmitting device is associated with said user), as required by independent claims 45 and 55.

Regarding issue 4, Applicants note that, even if each user is capable of having a separate GPS device, MacDoran does ***not*** disclose or suggest that each user has or should have a separate GPS device.

Regarding issue 5, the techniques cited by the Examiner as being disclosed by MacDoran (passwords, PIN's and biometric authentication) are techniques for attempting to authenticate an individual person. The tests cited by the Examiner, however, can falsely authenticate an individual who is actually an impostor, as would be apparent to a person of ordinary skill in the art. For example, fingerprints on artificial limbs are known to have been authenticated by fingerprint systems as belonging to an authorized user. The location of the authorized user may not be the same as the location of the electronic device in the system taught by MacDoran since an impostor who has acquired such an artificial limb and/or the authorized user's password may access an electronic device while the authorized user is at another location. In the present invention, the location of the authorized user is determined in order to prevent such false authentications. Thus, MacDoran does not disclose identifying the location of the authorized user.

Regarding issue 6, Applicants maintain that MacDoran's teaching that "the definition does not extend to individual users that operate an entity, because the invention does not have the ability to authenticate an individual person" clearly means that MacDoran does not disclose or suggest a system that can authenticate an individual user.

Regarding issue 7, Applicants note that MacDoran discloses identifying the location of the remote client machine, not identifying the location of an authorized user.

Regarding issue 8, in the text cited by the Examiner, Applicants could find no disclosure by MacDoran of "comparing a location of each identified potential *users*." MacDoran only discloses comparing a location of a client machine.

Regarding issue 9, as Applicants previously noted, biometric authentication systems may falsely authenticate a user by, for example, comparing a fingerprint on an artificial limb with a fingerprint image stored in a database. Thus, the authorized user may not be at the location where the biometric authentication is performed even if the biometric authentication (falsely) confirms the user's identity.

Thus, again, Li and MacDoran, alone or in combination, do not disclose or suggest identifying a location of an authorized person associated with said response; identifying a location where said response is received; and providing access to said user if said locations match, as required by independent claims 1, 16, 27, and 38, do not disclose or suggest identifying each registered person within a predefined distance of said requested device, as required by independent claims 39 and 49, do not disclose or suggest identifying said user by comparing a location of each identified potential users with a location where said biometric information was obtained, as required by independent claims 42 and 52, and do not disclose or suggest identifying said user and confirming said user requesting access to said device is physically present at the location of said requested device by determining a location of said transmitting device (wherein said transmitting device is associated with said user), as required by independent claims 45 and 55.

Claims 6, 17, 28, 40, 43, 50 and 53

Regarding claims 6, 17, and 28, the Examiner asserts that MacDoran discloses using a Global Positioning System (GPS) sensor to determine the location of

the signature provided by the remote client. Dependent claims 6, 17, and 28 require wherein said location of an authorized person is obtained using an *individual* global positioning system. As defined in the present invention, an individual global positioning system is a GPS device associated with *an individual (a user)* (page 3, lines 9-11, of the originally filed specification). MacDoran does not disclose or suggest that a GPS is associated with a user.

Similarly, dependent claims 43 and 53 require wherein said location of each identified potential user is obtained by identifying the location of an individual global positioning system associated with each of said identified potential users, and dependent claims 40 and 50 require wherein said step of identifying each registered person within a predefined distance of said requested device further comprises the step of identifying individual global positioning systems associated with registered persons within said predefined distance.

Thus, Li et al., MacDoran, and Meyer et al., alone or in combination, do not disclose or suggest wherein said location of an authorized person is obtained using an individual global positioning system, as required by claims 6, 17, and 18, do not disclose or suggest wherein said location of each identified potential user is obtained by identifying the location of an individual global positioning system associated with each of said identified potential users, as required by claims 43 and 53, and do not disclose or suggest wherein said step of identifying each registered person within a predefined distance of said requested device further comprises the step of identifying individual global positioning systems associated with registered persons within said predefined distance, as required by claims 40 and 50.

Claims 13, 24, 35, 41, 44, 51, and 54

Regarding claims 13, 24, and 35, the Examiner asserts that it would have been obvious to one having ordinary skill in the art to combine the wireless cellular phone as disclosed by Li with the global positioning system as disclosed by MacDoran in order to determine the location of an object or person with great precision and accuracy (MacDoran: col. 5, line 41-43).

Dependent claims 13, 24, 35, 44, and 54 require wherein said location of an authorized person is obtained by identifying the location of a *transmitting device* associated

with said authorized person. The GPS device disclosed by MacDoran is a *receiving device*, as would be apparent to a person of ordinary skill in the art.

Similarly, dependent claims 41 and 51 require wherein said registered person within a predefined distance of said requested device are identified by identifying transmitting devices associated with registered persons within said predefined distance.

Thus, Li et al., MacDoran, or Meyer et al., alone or in any combination, do not disclose or suggest wherein said location of an authorized person is obtained by identifying the location of a transmitting device associated with said authorized person, as required by dependent claims 13, 24, 35, 44, and 54, and do not disclose or suggest wherein said registered person within a predefined distance of said requested device are identified by identifying transmitting devices associated with registered persons within said predefined distance, as required by dependent claims 41 and 51.

Rejection Under 35 U.S.C. §103(a) as Being Unpatentable Over Li et al. in View of MacDoran et al., and Further in View of Meyer et al.

Independent Claims 1, 16, 27, 38, 39, 42, 45, 49, 52 and 55

Meyer et al. was also cited by the Examiner for its disclosure of asking the cell phone user "Do you have any more details on your location?" (Meyer: page 189, right column, lines 1-2; see, also, issue 10 above.) Applicants note that Meyer is directed to enhanced 9-1-1 service for wireless networks. Meyer does not disclose or suggest the identification of a user as described in the limitations of the independent claims.

Thus, Meyer does not disclose or suggest identifying a location of an authorized person associated with said response; identifying a location where said response is received; and providing access to said user if said locations match, as required by independent claims 1, 16, 27, and 38, does not disclose or suggest identifying each registered person within a predefined distance of said requested device, as required by independent claims 39 and 49, does not disclose or suggest identifying said user by comparing a location of each identified potential users with a location where said biometric information was obtained, as required by independent claims 42 and 52, and does not disclose or suggest identifying said user and confirming said user requesting access to said device is physically present at the location of said requested device by

determining a location of said transmitting device (wherein said transmitting device is associated with said user), as required by independent claims 45 and 55.

Claims 12, 23, 34, 48, and 58

Regarding claims 12, 23, 34, 48, and 58, the Examiner acknowledges that Li does not disclose using 911 techniques or querying the user about something at the location of a requested device or facility, but asserts that Meyer discloses asking the user of the cellphone "Do you have any more details on your location?" Dependent claims 12, 23, 34, 48, and 58 require wherein said location of an authorized person is obtained using enhanced cellular 911 techniques. Applicants could find no disclosure in Li, MacDoran, or Meyer, of obtaining the location of an authorized person using enhanced cellular 911 techniques.

Thus, Li et al., MacDoran, or Meyer et al., alone or in any combination, do not disclose or suggest wherein said location of an authorized person is obtained using enhanced cellular 911 techniques, as required by dependent claims 12, 23, 34, 48, and 58.

Conclusion

The rejections of the cited claims under section §103 in view of Li et al., MacDoran, and Meyer et al., alone or in any combination, are therefore believed to be improper and should be withdrawn. The remaining rejected dependent claims are believed allowable for at least the reasons identified above with respect to the independent claims.

The attention of the Examiner and the Appeal Board to this matter is appreciated.

Respectfully,

Date: April 7, 2005

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560

APPENDIX

1. A method for verifying the identity of a user, said method comprising the steps of:

issuing a challenge to said user;

receiving a response to said challenge from said user;

identifying a location of an authorized person associated with said response;

identifying a location where said response is received; and

providing access to said user if said locations match.

2. The method of claim 1, wherein said response is a password.

3. The method of claim 1, wherein said response is a pocket token.

4. The method of claim 1, wherein said response is a computer-readable card.

5. The method of claim 1, wherein said response is biometric information.

6. The method of claim 1, wherein said location of an authorized person is obtained using an individual global positioning system.

7. The method of claim 6, wherein said individual global positioning system includes a local verification system.

8. The method of claim 6, wherein said individual global positioning system is included in a portable device carried by said authorized user.

9. The method of claim 1, wherein said location where said response is received is obtained from an individual global positioning system associated with a requested device or facility.

10. The method of claim 1, wherein said location where said response is received is obtained from recorded information associated with a requested device or facility.

11. The method of claim 1, wherein said location of an authorized person is obtained using a triangulation technique.

12. The method of claim 1, wherein said location of an authorized person is obtained using enhanced cellular 911 techniques.

13. The method of claim 1, wherein said location of an authorized person is obtained by identifying the location of a transmitting device associated with said authorized person.

14. The method of claim 1, wherein said location of an authorized person is confirmed by querying said user about something at the location of a requested device or facility.

15. The method of claim 14, further comprising the step of identifying said user by applying speaker recognition techniques to an answer to said query.

16. A method for verifying the identity of a user, said method comprising the steps of:

receiving a response to a challenge from said user;

identifying a location of an authorized person associated with said response;

identifying a location where said response is received; and

providing access to said user if said locations match.

17. The method of claim 16, wherein said location of an authorized person is obtained using an individual global positioning system.

18. The method of claim 17, wherein said individual global positioning system includes a local verification system.

19. The method of claim 17, wherein said individual global positioning system is included in a portable device carried by said authorized user.

20. The method of claim 16, wherein said location where said response is received is obtained from an individual global positioning system associated with a requested device or facility.

21. The method of claim 16, wherein said location where said response is received is obtained from recorded information associated with a requested device or facility.

22. The method of claim 16, wherein said location of an authorized person is obtained using a triangulation technique.

23. The method of claim 16, wherein said location of an authorized person is obtained using enhanced cellular 911 techniques.

24. The method of claim 16, wherein said location of an authorized person is obtained by identifying the location of a transmitting device associated with said authorized person.

25. The method of claim 16, wherein said location of an authorized person is confirmed by querying said user about something at the location of a requested device or facility.

26. The method of claim 25, further comprising the step of identifying said user by applying speaker recognition techniques to an answer to said query.

27. A system for verifying the identity of a user, comprising:

a memory that stores computer readable code; and

a processor operatively coupled to said memory, said processor configured to:

receive a response to a challenge from said user;

identify a location of an authorized person associated with said password;

identify a location of where said response is received; and

provide access to said user if said locations match.

28. The system of claim 27, wherein said location of an authorized person is obtained using an individual global positioning system.

29. The system of claim 28, wherein said individual global positioning system includes a local verification system.

30. The system of claim 28, wherein said individual global positioning system is included in a portable device carried by said authorized user.

31. The system of claim 27, wherein said location where said response is received is obtained from an individual global positioning system associated with a requested device or facility.

32. The system of claim 27, wherein said location where said response is received is obtained from recorded information associated with a requested device or facility.

33. The system of claim 27, wherein said location of an authorized person is obtained using a triangulation technique.

34. The system of claim 27, wherein said location of an authorized person is obtained using enhanced cellular 911 techniques.

35. The system of claim 27, wherein said location of an authorized person is obtained by identifying the location of a transmitting device associated with said authorized person.

36. The system of claim 27, wherein said location of an authorized person is confirmed by querying said user about something at the location of a requested device or facility.

37. The system of claim 36, wherein said processor is further configured to identify said user by applying a speaker recognition technique to an answer to said query.

38. An article of manufacture for verifying the identity of a user, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to receive a response to a challenge from said user;

a step to identify a location of an authorized person associated with said response;

a step to identify a location where said response is received; and

a step to provide access to said user if said locations match.

39. A method for identifying a user requesting access to a device, said method comprising the steps of:

receiving biometric information from said user;

identifying each registered person within a predefined distance of said requested device; and

identifying said user from among said identified persons using said biometric information.

40. The method of claim 39, wherein said step of identifying each registered person within a predefined distance of said requested device further comprises the step of

identifying individual global positioning systems associated with registered persons within said predefined distance.

41. The method of claim 39, wherein said step of identifying each registered person within a predefined distance of said requested device further comprises the step of identifying transmitting devices associated with registered persons within said predefined distance.

42. A method for identifying a user requesting access, said method comprising the steps of:

receiving biometric information from said user;

identifying a list of potential users based on said biometric information; and

identifying said user by comparing a location of each identified potential users with a location where said biometric information was obtained.

43. The method of claim 42, wherein said location of each identified potential user is obtained by identifying the location of an individual global positioning system associated with each of said identified potential users.

44. The method of claim 42, wherein said location of each identified potential user is obtained by identifying the location of a transmitting device associated with each of said identified potential users.

45. A method for identifying of a user requesting access to a device, said method comprising the steps of:

receiving a communication from a transmitting device associated with said user;

identifying said user using a voice recognition system; and

confirming said user requesting access to said device is physically present at the location of said requested device by determining a location of said transmitting device.

46. The method of claim 45, wherein said transmitting device is a cellular telephone.

47. The method of claim 46, further comprising the step of confirming that said user is using a cellular telephone associated with said user using caller identification techniques.

48. The method of claim 47, wherein confirming step further comprises the step of determining the location of said cellular telephone using enhanced cellular 911 techniques.

49. A system for identifying a user requesting access to a device, comprising:

a memory that stores computer readable code; and

a processor operatively coupled to said memory, said processor configured to:

receive biometric information from said user;

identify each registered person within a predefined distance of said requested device; and

identify said user from among said identified persons using said biometric information.

50. The system of claim 49, wherein said registered persons within a predefined distance of said requested device further are identified by identifying individual global positioning systems associated with registered persons within said predefined distance.

51. The system of claim 49, wherein said registered person within a predefined distance of said requested device are identified by identifying transmitting devices associated with registered persons within said predefined distance.

52. A system for identifying a user requesting access, comprising:

a memory that stores computer readable code; and

a processor operatively coupled to said memory, said processor configured to:

receive biometric information from said user;

identify a list of potential users based on said biometric information; and

identify said user by comparing a location of each identified potential users with a location where said biometric information was obtained.

53. The system of claim 52, wherein said location of each identified potential user is obtained by identifying the location of an individual global positioning system associated with each of said identified potential users.

54. The system of claim 52, wherein said location of each identified potential user is obtained by identifying the location of a transmitting device associated with each of said identified potential users.

55. A system for identifying of a user requesting access to a device, comprising:

a memory that stores computer readable code; and

a processor operatively coupled to said memory, said processor configured to:

receive a communication from a transmitting device associated with said user;

identify said user using a voice recognition system; and

confirm said user requesting access to said device is physically present at the location of said requested device by determining a location of said transmitting device.

56. The system of claim 55, wherein said transmitting device is a cellular telephone.

57. The system of claim 56, wherein said processor is further configured to confirm that said user is using a cellular telephone associated with said user using caller identification techniques.

58. The system of claim 57, wherein said processor is further configured to determine the location of said cellular telephone using enhanced cellular 911 techniques.

Receipt in the USPTO is hereby acknowledged of:

Transmittal Letter – (Original & 1 copy)
Notice of Appeal - (Original & 1 copy)

February 3, 2005
Serial No.: 09/437,352
YO999-411
1500-61 (KMM)

PTO/SB/31 (02-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

COPY

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES	Docket Number (Optional) YO999-411

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Assistant Commissioner for Patents, Washington D.C. 20231" on February 3, 2005.

Signature: Tina Maurice

Typed or printed name: Tina Maurice

In re Application of: Kanevsky et al.

Application Number	Filed
09/437,352	November 9, 1999

For: Methods and Apparatus for Verifying the Identity of a User Requesting Access Using Location Information

Group Art Unit	Examiner
2132	Cas P. Stulberger

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 1.17(b)) $ 500.00.

- ☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $_____.
- ☐ A check in the amount of the fee is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Commissioner has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of this sheet.
- ☑ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0510. I have enclosed a duplicate copy of this sheet.
- ☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record.
- ☐ attorney or agent acting under 37 CFR 1.34(a). Registration number if acting under 37 CFR 1.34(a)._____.

Kevin M. Mason
Signature

Kevin M. Mason
Typed or printed name

February 3, 2005
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of 1 forms are submitted.